

④ (2) 文献

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-227152

(43)Date of publication of application : 03.09.1993

(51)Int.Cl.

H04L 9/06

H04L 9/14

H04L 7/00

H04L 7/10

(21)Application number : 04-290804

(71)Applicant : MOTOROLA INC

(22)Date of filing : 05.10.1992

(72)Inventor : HARDY DOUGLAS A  
LEWIS LESLIE K

(30)Priority

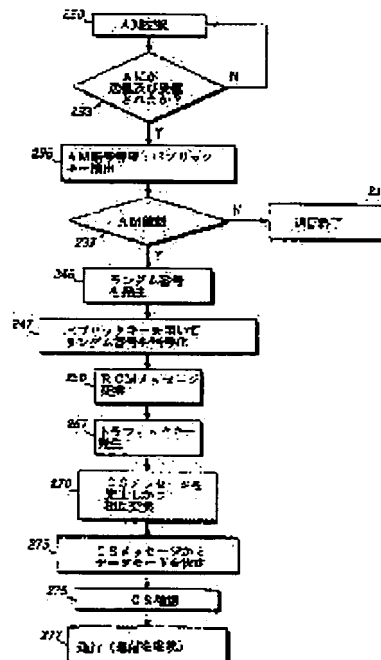
Priority number : 91 777870 Priority date : 16.10.1991 Priority country : US

## (54) METHOD AND DEVICE FOR ESTABLISHING SECURITY COMMUNICATION LINK

(57)Abstract:

PURPOSE: To attain security communication among various tapes of user devices, using different encryption algorithm and encryption keys.

CONSTITUTION: This security communication equipment includes a controller that uses any of common encryption algorithm sets for transmission and reception terminals to automatically select one of data encryption devices. A transmitter for encryption data and a receiver for encryption data are connected to a plurality of encryption devices. The controller automatically decides an encryption device to be adopted. The method to set up a security communication link includes a 1st message exchange stage deciding a common key production and the encryption method and a stage to confirm the validity of the communication terminal security through the comparison with other common message. Other message exchange stage for a traffic key, a state of inter-exchanging other message for synchronization confirmation and synchronization of security communication between terminals and a state starting the security communication are also used.



## LEGAL STATUS

[Date of request for examination] 30.09.1999

[Date of sending the examiner's decision of rejection] 08.04.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-227152

(43)公開日 平成 5 年(1993) 9 月 3 日

(51)Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
9/14				
7/00	A	7928-5K		
7/10		7928-5K		
		7117-5K		
			H 0 4 L 9/ 02	Z

審査請求 未請求 請求項の数 3 (全 10 頁)

(21)出願番号 特願平4-290804

(22)出願日 平成 4 年(1992)10 月 5 日

(31)優先権主張番号 7 7 7, 8 7 0

(32)優先日 1991年10月16日

(33)優先権主張国 米国 (U S)

(71)出願人 390009597

モトローラ・インコーポレイテッド  
MOTOROLA INCORPORATED

アメリカ合衆国イリノイ州シャンパーグ、  
イースト・アルゴンクイン・ロード1303

(72)発明者 ダグラス・エイ・ハーディ

アメリカ合衆国アリゾナ州85204、メサ、  
イースト・ゲイブル・アベニュー 2207

(72)発明者 レスリー・ケイ・ルイス

アメリカ合衆国アリゾナ州85260、スコッ  
ツデイル、イースト・ヴォルテア・アベ  
ニュー 8007

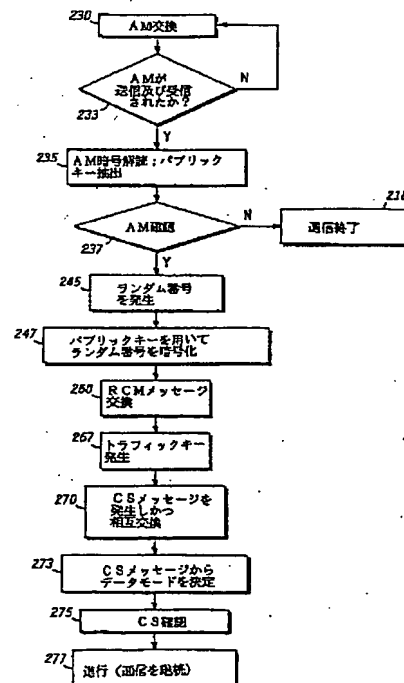
(74)代理人 弁理士 池内 義明

(54)【発明の名称】 機密通信リンクを確立する方法および装置

(57)【要約】

【目的】 異なる暗号アルゴリズム、暗号キーを用いる種々のタイプのユーザ機器間での機密通信を可能にする。

【構成】 機密通信用の装置は、送信および受信ターミナルに共通の暗号化アルゴリズムの1つを利用して、データ暗号化装置の1つを自動的に選択するコントローラを含む。暗号化データの送信機と、暗号化データの受信機が、複数の暗号化装置に結合される。コントローラは採用する暗号化装置を自動的に決定する。機密通信リンクを確立する方法は、共通のキー発生と暗号化方法を決定する第1メッセージ交換段階と、別の共有メッセージを比較して通信ターミナル機密の有効性を確認する段階とを含む。また、トラフィックキーのためのさらに別のメッセージの交換段階と、ターミナル間の機密通信の同期と同期確認用の別のメッセージを相互に交換する段階と、機密通信の開始段階とが用いられる。



## 【特許請求の範囲】

【請求項1】 第1(103, A)および第2(109, B)ターミナル間に機密通信リンクを確立する方法であって、前記ターミナル(103, A, 109, B)が：両ターミナル(103, A, 109, B)内で使用可能な暗号化装置と通信モードとに関する情報を含む第1メッセージを交換する段階(211)；少なくとも1つのターミナル(103, A, 109またはB)において、共通のキー発生および暗号化の方法と、共通データ速度とを選択する段階(219, 221, 222)；ユーザの認証情報を含む第2メッセージを交換する段階(230)；トラフィック・キーを形成するためのデータを与える第3メッセージを交換する段階(250)；機密通信を同期させる第4メッセージを交換する段階(270)；および機密通信を開始する段階(277)；を含む手順に従うことを特徴とする機密通信リンクを確立する方法。

【請求項2】 ターミナル(103, A, 109, B)間に機密通信リンクを確立する方法であって、各ターミナル(103, A, 109, B)が：暗号化および解読機能を備えたアクセス・ドメインおよび機能メッセージを交換する段階(211)；認定されたユーザの認証データ、認定されたユーザのパブリック・キーを備えた認証メッセージを交換する段階(230)；第1乱数を含む第1乱数部メッセージを送り、第2乱数を含む第2乱数部メッセージを受け取り、トラフィック・キーを形成する段階(250)；暗号化同期メッセージを相互に交換する段階(270)；および機密情報相互交換を開始する段階(273, 275, 277)；を具備する手順に従うことを特徴とする機密通信リンクを確立する方法。

【請求項3】 いくつかの暗号化アルゴリズムのいずれかを用いて機密通信リンクを確立する装置(100)であって：異なる暗号化アルゴリズムを利用する複数のデータ暗号化手段(KG1, . . . , KGN)；暗号化されたデータを送る、前記複数の暗号化手段(KG1, . . . , KGN)に結合された送信手段(103または109, AまたはB)；暗号化されたデータを受け取る、前記複数の暗号化手段(KG1, . . . , KGN)に結合された受信手段(109または103, BまたはA)；およびある機密通信に関して、前記複数の暗号化手段(KG1, . . . , KGN)のどれを採用するかを自動的に決定する制御手段(210)；を組み合わせることを特徴とする機密通信リンクを確立する装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、保安または機密通信(secure communication)の改善された手段と方法とに関する。さらに詳しくは、異なった暗号アルゴリズムお

よび／または暗号キーを採用している様々な種類のユーザ装置間の機密通信に関する。

## 【0002】

【従来の技術】 民間および軍事のユーザ間での機密通信に対する必要性が増大するのに合わせて、さまざまな暗号化技術とそれに対応する装置とが開発されてきた。無認可の(unauthorized)データ傍受が公益を害したり、個人の事業上の利益を害することがあるので、産業上、財政上、政府、警察、加入者媒体やその他の商業的活動および民間活動のための機密上の要件がより厳格になることにより、上記の必要性が強化されている。

【0003】 通常の暗号化されたデータには、コンピュータによる記録、電話での会話やその他の音声データ、遠隔測定データ、ファクシミリ送信、全地球測位システム(Global Positioning System)や加入者情報配布システムを含むさまざまな発信源からの地上と衛星との通信および衛星間の通信がある。データを暗号化する動機付けとしては、より均等なデータの混合(たとえば、「1」と「0」の不均衡な未暗号化列ではなく、「1」と「0」とが均等に混合された暗号データの通信)を促進することによる改善された信号対雑音比、加入者料金の強制、特権を与えられている会話のプライバシー、国家の機密事項およびコンピュータ犯罪を防ぎ同時に機密性を確保してユーザの認証を守るための商取引の完全性の維持などがある。

【0004】 情報監視や暗号解読法が発達したことにより、新しい暗号化アルゴリズムやそれに対応する装置の生産が誘導された。一例としてあげると、ただしこれに限らないが、現在広く用いられているいくつかのクラスの暗号化法には、いずれも米国商務省により発行された連邦情報処理規格(Federal Information Processing Standard Publications) FIPS 46-1に記述されるデータ暗号化規格(Data Encryption Standard - DES)「データ暗号化規格」と、FIPS 81の「DES動作モード」があげられる。

【0005】 これらの多様な暗号化装置とアルゴリズムに共通の要素が、認可を受けた送信者および受信者が、暗号化を行いその後で意図されたメッセージを解読することができるある形態の暗号キー情報を共有するために必要とされる。

【0006】 電話などの機密通信のための従来の技術のパブリック・キー暗号化システムの欠点は、パブリック・キー・データ暗号化および解読が非常に速度の遅い処理であるということである。従って、パブリック・キー暗号化法は、より高速の暗号化技術のためのトラフィック・キーのような少量の情報の送信に用いられることが多く、無線チャンネルや電話回線などの公共の送信媒体において機密的な方法で用いられる。

【0007】 リアルタイムの双方向通信のための暗号化方法には、上記のFIPS 46-1および81に開示さ

れているさまざまな暗号化技術や、このような装置を供給する企業により開発されたその他の技術が含まれる。これらの方法により、双方がデータの暗号化のための適切なトラフィック・キーを有するかあるいはアクセスすることができれば、優れたデータの完全性を図ることができる。通常、この方法は、さまざまなデジタルまたはアナログ形式の入力データから形成されたデジタル・データのブロック上で動作する。

#### 【0008】

【発明が解決しようとする課題】ときには、複数の通信チャンネルを用いねばならないこともある。たとえば、逐次であろうと並列的であろうと2者以上の発信者と受信者とが関わる場合がそうである。すべてのユーザが同じ装置や、同じ暗号キーまたはアルゴリズムを持っていないことも多い。このような場合、暗号キーまたは暗号化アルゴリズムおよび装置が異なる余剰な装置が、各発信場所または受信場所が必要になることがある。このために通信装置や費用がよけいにかかる。さらに通信用装置の種類が可動式または携帯式であることが必要な場合は、複数の別個の機密通信用システムに合わせるために必要な電力要件、重量および大きな寸法を受け入れることはできない。

【0009】1台の通信用ターミナルで複数の暗号化技術に対応しても、ユーザが他者の機能を知ることや、適切な機密通信装置を手動でユーザが選択することが必要になることもある。このため、採用される機密アルゴリズムやハードウェアの詳細に対するユーザの知識を増やし、認可されたユーザの情報をより多くの個人に広め、さらに機密通信を開始するために必要な詳細な構造に關知するユーザを増やすことになるので通信の機密性が損なわれることもある。このために機密通信リンクに影響を与えるエラーの危険性が増す。

【0010】必要とされるのは、単独の装置内で複数の暗号化アルゴリズムおよび暗号キーに対応してリアルタイムの機密通信を迅速に行い、認可を受けた自己同期通信を多様な加入者間で確立および維持することができるようにする手段である。装置は小型軽量で、電力要件が低いことがさらに望ましい。

#### 【0011】

【課題を解決するための手段】本発明により、多様な暗号化システム間で暗号通信を実行するための新規の方法と装置とが開示される。

【0012】機密通信用リンクを確立する方法は、両ターミナル内で使用することのできる暗号化装置と通信モードに関する情報を含む第1メッセージを交換する段階と、少なくとも1つのターミナル内で共通キーの発生および暗号化の方法と、共通データ速度とを選択する段階と、ユーザ認証情報を含む第2メッセージを交換する段階と、トラフィック・キーを形成するためのデータを提供第3メッセージを交換する段階と、機密通信を同

期させるための第4メッセージを交換する段階と、機密通信を開始する段階とを含む。

【0013】機密通信のための装置には、異なる暗号化アルゴリズムを利用する複数のデータ暗号化手段と、暗号化されたデータを送信する、前記の複数の暗号化手段に結合された送信手段と、暗号化されたデータを受信する、前記の複数の暗号化手段に結合された受信手段と、前記の複数の暗号化手段のうちのどれを特定の機密通信のために採用するかを自動的に決定する制御手段とが含まれる。

【0014】本発明の上記およびその他の特徴と利点とは、以下の詳細な説明と添付の図面とからさらによく理解されるであろう。

#### 【0015】

【実施例】ここで用いられる「暗号化」という言葉 (encryption, enciphering, encoding) は、生のテキストのメッセージを機密メッセージに変換することを意味し、「解読」(decryption, deciphering, decoding) はその反対の処理を意味する。

【0016】図1は、電話ネットワーク120、電話回線107、たとえば機密電話などの機密通信用ターミナル103、109を備えた機密通信システム100を示す。動作においては、音声データが機密通信用ターミナル103、109のいずれかにおいてデジタル化される。ここでは「電話」または「通信用ターミナル」という言葉は、音声情報、ファクシミリ、映像、コンピュータ・データ、グラフィック・データおよびその組合せの情報を含み、ただしそれに限定されない情報を送信する任意の装置を含むものとし、「音声」、「データ」または「音声データ」という言葉はこれらとその他すべての種類の送信可能な情報を含むものとする。

【0017】入力データは、ターミナル103または109で暗号化され、その後で、電話回線107および電話ネットワーク120を介して、順次、たとえばもう1つの機密通信用ターミナル109または103に送られる。ここで、暗号化とデジタル化の動作が逆に実行されて、元の入力データに相当する生のテキストのデータが作成される。無線リンク、パケット交換データ・ネットワーク、専用回線またはその他の通信用チャンネルなどの別の送信媒体を、電話回線107と電話ネットワーク120の代わりに用いても有用である。伝統的に、機密通信用ターミナル103、109に外付けあるいは内蔵することのできるモデムを用いて、電話回線またはその他の通信用リンク上でデジタル・データ・ストリームを通信する。

【0018】本発明は、ターミナル103、109のいずれか一方あるいは両方の中に、両ターミナルが理解することのできるいくつかの可能なプロトコルの内の1つに従ってメッセージを暗号化および解読する手段と方法とを設けて、特性やプロトコルの異なるターミナル同士

が互いに通話を行うことができるようにすることにより従来の技術の問題を克服する。好適な実施例においては、プロトコルの選択は自動でありユーザにとって透過的 (transparent) な形で実行される。好適な階層のプロトコルが含まれていることが望ましい。このように、本発明の多重プロトコル・ターミナルは、他の同じでないターミナルと通信することができる。

【0019】図2は、機密通信用ターミナル103（および/または109）内のキー管理データ・ベース210の一例を概略図で示したもので、複数の暗号化キーと装置KG1ないしKGNが配置されている。KG1ないしKGNは、所定のN個のアルゴリズムのうちの1つに従い、選択された特定のアルゴリズムに適したキーを用いてメッセージの暗号化/解読を行う。制御手段215は、相互接続部220により複数の暗号化キーと装置KG1ないしKGNに結合されており、特定の暗号化アルゴリズムを制御手段215により選択的に採用することができる。各機密通信用ターミナル103、109には、1対のキー管理データ・ベース210が含まれ、一方は情報を暗号化して送信することを専門に行い、もう一方は、情報を受信して解読することを専門に行う。1つのキー管理データ・ベース210で両方の機能を行うこともでき、それが好ましい。2台（またはそれ以上）の通信用ターミナル103、109のうち1台だけが、複数の暗号化キーおよび装置KG1ないしKGNを有する必要がある。もう1台のターミナルは、多重装置ターミナルにあるもののうち1つだけを持っていればよい。

【0020】機密通信を開始することができるようにするには、ターミナル103、109を初期化しなければならない。本発明の好適な実施例により、初期化は、手動キー管理モードまたはパブリック・キー管理モードの2つのモードのいずれか一方により行う。パブリック・キー管理モードを用いると、その特定の通信用の独自の暗号化キーの対を機密通信用ターミナルに物理的に運搬する（手で運ぶなど）不便さを避けることができる。

【0021】図3は、ターミナルA、B（たとえばターミナル103、109）間の機密通信を、本発明によるパブリック・キー・モードで自動的に開始するためのメッセージ配列の一部を示す。図3に概略的に示されるように、パブリック・キー管理モードには、4つのメッセージの交換が含まれる。これらは (i) アクセス・ドメインおよび機能 (Access Domain and Capabilities: AD&C) メッセージ211、(ii) 認証メッセージ (Authentication Message: AM) 230、(iii) 乱数部メッセージ (Random Component Message: RCM) 250および (iv) 暗号化同期 (Cryptographic Synchronization: CS) メッセージ270である。これらのメッセージはそれぞれ、一連のバイトからなる所定の長さであることが望ましい。各バイトには、特定の種類（たとえば使用可能な暗号化装置、モデムの種類な

ど）の情報が含まれていることが望ましく、たとえば、適切なバイト群を結びつけてメッセージを形成することなどにより、完全なメッセージが形成される。

【0022】アクセス・ドメインおよび機能 (AD&C) メッセージ211は、この場合、以下のことを実行する。すなわち、キー管理モードの選択、選択されたキー発生器 (KG) アルゴリズムの選択、ターミナルの認可の認定および他のターミナル機能（たとえばデータ速度）。図4は、図3のAD&Cメッセージ211を用いて本発明によりデータ速度と暗号化アルゴリズムの適合を行う方法200を示す流れ図である。

【0023】図4に示されている方法200は、ブロック211でアクセス・ドメインおよび機能 (AD&C) メッセージを交換する段階と、次のデータ速度をチェックする段階213、適切なデータ速度が識別されたか否かを判定する決定段階216およびすべてのデータ速度がチェックされたか否かを確認する段階217を含む反復ループ213、216、217と、決定段階216によりデータ速度の整合または適合が検出されたときにループ219、221、222に進む段階、または適合が発見できずにすべてのデータ速度がチェックされた場合に通信を終了させる段階218を備えて構成される。ループ219、221、222には、次の暗号化アルゴリズムをチェックする段階219と、適切な暗号化アルゴリズム (すなわち両ターミナルに共通のアルゴリズム) が識別されたか否かを判定する決定段階221と、すべての暗号化アルゴリズムがチェックされたことを確認する段階222とが含まれ、その後、決定段階221が暗号化アルゴリズムの適合を検出した場合に動作を進める段階224と、適合を発見できずにすべての暗号化アルゴリズムをチェックし終った場合に通信を終了させる段階218とが続く。

【0024】KG1およびDESと示されているキー発生器がただ2つだけあり、KG1およびDESが両方とも2つのターミナルに共通である場合には、DESキーが好まれる状態が与えられている場合を一例として考える。ただしこれに限られるものではない。この状態では、方法200は、4つの可能な結果のいずれかでAD&Cメッセージの交換を終了する。すなわち：(i) 2つのターミナル間で適合が発見できなかった場合に、呼は終了される；(ii) 2つのターミナルにKG1モードだけが共通の場合、KG1キー発生器が用いられる；(iii) 2つのターミナルにDESキー発生器だけが共通の場合、DESキー発生器が用いられる；(iv) DESモードとKG1モードの両方が両ターミナルに共通の場合、DESキー発生器が用いられる。キー発生器機能のリストがもっと長い場合にも同様の結果が当てはまり、最も好適な共通の状況のキー発生器がその後の通信のために選択される。キー発生器の好適な順序は、ターミナルにあらかじめプログラミングされているか、あ

るいはAD&Cまたは他のメッセージの一部として送信される。

【0025】ターミナルの機能は、メッセージ全体の中で、特定のバイトまたは（たとえば8個の）ビット群により示される。特定のバイトの特定のビット群を用いて、所定のプロトコルによりある機能を示す。たとえば、キー発生器機能バイトの先頭ビットは、占有の(proprietary)キー発生器のための機能を表わし、次のビットはDESタイプのキー発生器の機能を表わすように選択することができる。データ速度機能などに関しても、同様の用法を採用することができる。

【0026】図5は、ターミナル認定の有効性を決定し、トラフィック・キーを設定し、暗号化/解読のプロセスを同期させる、図3の第2、第3および第4メッセージの交換を示す流れ図である。以下の段階が本発明により実行される。すなわち認証メッセージ(AM)の交換230、乱数部メッセージ(RCM)の交換250および暗号化同期(CS)メッセージの交換270である。機密通信を行う(ブロック277)ための確認(ブロック275)があることも望ましい。

【0027】図5は、認証メッセージ(AM)の交換の段階(ブロック230)、AM交換の確認の段階(ブロック233)、AM解読とパブリック・キー抽出の段階(ブロック235)およびAM確認の段階(ブロック237)を含むループ230、233、235、237と、AM確認が失敗したときに通信を終了する段階218とを具備する。これらの段階の次に、乱数発生段階(ブロック245)と、たとえばパブリック・キー暗号化を用いた乱数暗号化の段階(ブロック247)と、乱数部メッセージ交換の段階(ブロック250)と、トラフィック・キー発生の段階(ブロック267)と、暗号化同期メッセージの発生と送信の段階(ブロック270)と、データ・モード決定の段階(ブロック273)と、暗号化同期確認の段階(ブロック275)と、通信の継続の段階(277)とが続く。

【0028】AM交換の段階(ブロック230)では、認定されたユーザ認証情報と、認定されたユーザ・パブリック・キーと、認定された情報の有効期限とを識別する情報が提供される。このメッセージは、パブリック・キー暗号法を用いて処理され、当技術では既知の手段によりメッセージの暗号化および解読を行う。

【0029】各ターミナルでは乱数が発生され(ブロック245)、たとえばAMで受け取られたパブリック・キーを用いて暗号化された後で、他のターミナルに送られる。このため、交換(ブロック250)される各乱数部メッセージ(RCM)には、交換されたRCMを発した通信用ターミナルにより発生された乱数が含まれる。この乱数は、機密通信システムにおいて採用されるキー発生器のいずれかのためのトラフィック・キーを提供するのに十分な長さでなければならない。この第1

乱数もまた、発信ターミナルに記憶され、他のターミナルから返された乱数部メッセージから解読された第2乱数と組み合わせられる(ブロック267)。組み合わせられた第1および第2乱数が、第3乱数を形成する。このとき、もう一方のターミナルでも同じことが起こっており、受け取られた(第1)乱数が内部で発生された(第2)乱数と組み合わせられて、同じ第3乱数が形成される。第3乱数は、両ターミナルのために選択された(図4のブロック221)キー発生器のためのトラフィック・キーとして用いられ、最上位ビットからその中にロードされる。トラフィック・キー内の用いられなかったビットはすべて廃棄され、単一の装置が、変化するトラフィック・キー長を発生して、キー管理データ・ベース210(図2参照)内で複数のキー発生器の要件が異なる場合にも対応することができる。第1乱数は、たとえば、受け取られた認証メッセージ(ブロック230)に含まれる認定されたユーザ・パブリック・キーを用いて、RCMに組み込まれ交換される(ブロック250)前に暗号化される(ブロック270)。もう一方のターミナルから来た第2乱数にも、同じことが起こる。第1および第2乱数値を組み合わせる(ブロック267)方法として、当技術で既知のようにビット形式で乱数群を排他的OR処理することにより容易に実行することのできるモジュロ2の加算(modulo-two addition)があげられる。しかし、当技術で既知の二進数を組み合わせる他の手段と方法とを用いることもできる。

【0030】暗号化同期(CS)メッセージ270は、トラフィックの様式(音声、データなど)の情報と、必要に応じた暗号情報と、KG同期確認とを伝達する。線形帰還シフト・レジスタ(linear feedback shift register—LFSR)を、暗号化装置の一部として用いることもできる。線形帰還シフト・レジスタは、開始値すなわちシードを必要とする。シードは、CSメッセージ270の一部として必要になることがある暗号情報の一例である。LFSRは、当技術では既知である。

【0031】KG同期確認のための好適な方法は、既知のまたはチェック・データ・パターンの暗号化されたものであるデータを送信することである。これらのデータは、LFSRにシードをロードして、送信側のLFSRとKGとを同期させ、その後で送信側のLFSRおよびKGを用いてシードおよびチェック・パターンを暗号化することにより発生される。これらの受信されたデータが、受信側の機密通信用ターミナルにより解読されると、受信されたシードは受信側のLFSRにロードされ、チェック・データ・パターンは、そこに記憶されているものと比較される。このパターン間の適合(match)が、機密通信用ターミナルの暗号化同期を示す。

【0032】このようにこれらの段階により、複数の暗号化機能を有する機密通信用ターミナルが、自動的に(i)所定の暗号化モードの階層から適切な暗号化モー

ドを選択して、(i i) 共通のデータ速度を選択し、  
(i i i) 適切なターミナルの識別とユーザの認可とを  
実行し、(i v) パブリック・キーまたは他の方法を介  
してトラフィック・キーを交換し、(v) 暗号化通信の  
同期と確認とを実行することが可能になる。

【0033】上記の段階は、大半がオペレータの目に見  
えない (transparent) 方法で実行され、システムの機密  
性を増大させ、しかもオペレータは詳細な暗号化手順や  
方法に関する知識はより少なくて済む。

【0034】手動キー管理モードにおいては、呼の設定  
手順は、図3および図4のアクセス・ドメインおよび機  
能 (AD & C) メッセージ211および図3および図5  
の暗号化同期 (CS) メッセージ270の交換から構成  
される。

【0035】図4のアクセス・ドメインおよび機能 (A  
D & C) メッセージ211は、どのキー管理モードを採  
用すべきか、どのKGアルゴリズムを選択すべきか、手  
動キー・データ・ベース内のどのトラフィック・キーを  
用いるべきか、またその他のターミナル機能を決定する  
ための情報を提供する。

【0036】暗号化同期メッセージ270の交換 (図  
5) は、トラフィック・モード (音声、データなど) 線  
形帰還シフト・レジスタのシード値および/またはKG  
開始点を特定する情報を与えて、さらにKG同期の確認  
を可能にする。

【0037】<具体化例>以下に示すのは、本発明の手  
段と方法の一例である。図6は、ターミナル103 (お  
よび/または109) に類似の機密通信用ターミナル6  
00を示し、モデム610が電話回線またはその他の通  
信用システム605と通信を行い、マイクロプロセッサ  
・コントローラ620に接続されている。マイクロプロ  
セッサ・コントローラ620は、キー管理データ・ベ  
ース630に結合され、さらに633と識別されるキー発  
生器KG1と、637と識別されるKG (たとえばDES)  
と、スイッチ640と、音声またはデータ・リンク  
645とに結合されている。スイッチ640は、キー発  
生器633、637のどちらが音声またはデータ・リン  
ク645をマイクロプロセッサ・コントローラ620、  
モデム610および通信用システム605に接続するた  
めに使用されるかを決定する。

【0038】図7は、AD & Cメッセージ211 (図3  
および図4) のKG機能バイト710およびモデム速度  
機能バイト720を示し、キー発生の様式と、データ速  
度と、与えられた機密通信用ターミナル103、109  
(図1) により支援されるフォーマットとを示す。これ  
らの例では、使用されないビットには“RES”と印が  
付けられ、使用されるビットと共に完全な機能バイト (C  
apabilities bytes) を形成する。優先順位が最も高いビ  
ットは、“RES”と記されていない最も左側のビット  
である。そのため、KG機能バイト710内では、優先

順位が最も高いキー発生器はDESで、KG1は次に優  
先順位が高いキー発生器となる。同様に、データ速度の  
優先順位は、当技術では既知の標準のデータ速度によ  
り、96D (最高) から48V (最低) までの範囲となる。

【0039】第1段階は、AD & Cメッセージ211  
(図3および図4参照) の発生であり、これは図7の7  
10、720のようにバイト群から構成され、AD & C  
メッセージ211を発信する装置の機能を記述する。次  
にAD & Cメッセージが交換され (図2のブロック21  
1)、マイクロプロセッサ・コントローラ620に渡さ  
れる。ここでメッセージは、段階213、216、21  
7、219、221、222および224のように分解  
され、2つの機密通信用ターミナル間の対応する機能を  
決定する。対応関係の決定ができない場合は、通信は終  
了される (ブロック218)。適合すると、通信は進行  
する (ブロック224)。

【0040】KG1およびDESと示されている2つの  
可能なキー発生器だけを考慮した場合は、DESキー発  
生器に、両者が2つのターミナルに共通である (図7の  
バイト710のように) 場合に、優先的な状況を与える  
と、AD & Cメッセージの交換 (ブロック211) は前  
述のように4つの可能な結果のいずれかで終了する。

【0041】初期のモデム速度は、呼を起こした機密タ  
ーミナルにより設定される。このモデム速度は、両方  
の機密ターミナルに共通の別のモデム速度に変更するこ  
ともできる。

【0042】マイクロプロセッサ・コントローラ620  
(図6) は次に、モデム610を介して、第1認証メッ  
セージ (AM) を送り、第2AMを受け取る (図5のブ  
ロック230)。受け取られたAMは、処理され (プロ  
ック235、237)、パブリック・キーを解釈して、  
AMを確認する (verify)。AMが確認されない場合は、  
プロセッサは所定回数再試行を行うことができ、それ  
でも確認できない場合は、図5のブロック218のように  
通信を終了する。

【0043】次にマイクロプロセッサ・コントローラ6  
20は、キー管理データ・ベース630 (図2の210  
に類似のもの) から、キー発生器KG1ないしKGNの  
うちの1つを採用して、乱数を発生し (図5のブロック  
245)、この乱数は受け取られたAMから解釈された  
(ブロック235) パブリック・キーを用いて暗号化  
(ブロック247) される。暗号化された乱数とその他  
のデータが組み合わされて、乱数部メッセージ (random  
component message: RCM) が形成され、このメッ  
セージはRCMのためのモデム610を介して遠隔地の  
(もう一方の) 機密通信用ターミナルから交換される。  
受け取られたRCMから得られた乱数は、その前に発生  
された乱数 (ブロック245) と組み合わせられて、AD  
& Cメッセージから決定されたキー発生器のためのトラ

フィック・キーを形成する。乱数は、たとえば2個の二進数を排他的OR処理することにより実現される演算であるモジュロ2の演算を用いて加算することにより組み合わせることができる。

【0044】その結果得られる(第3)の乱数を、AD&Cメッセージの交換(ブロック211)により選択されたKG内に、最上位ビットからロードする。

【0045】マイクロプロセッサ・コントローラ620は、送信側の線形帰還シフト・レジスタのためのシードとして用いられる別の乱数を発生する。チェック・パターンが暗号化されて、CSメッセージの一部として送信される(ブロック270)が、これには遠隔地の(もう一方の)ターミナルの受信側LFSRおよび/またはKGのためのシード(複数)も含まれている。遠隔のターミナルから受け取られたCSメッセージ(ブロック270)には、第1(発信側の)機密通信用ターミナルの受信側LFSRおよび/またはKGにより用いられるシードが含まれる。これは受信されたCSメッセージから解読され、受信されたチェック・パターンを解読するために用いられる。遠隔のターミナルにおいても同様の動作が実行される。チェック・パターンが適切に解読され

(ブロック275)、記憶されたデータ・チェック・パターンに照合されると、望ましいメッセージの機密通信が進行される(ブロック277)。チェック・パターンの解読がうまく行かない場合、キー発生器に再度乱数がロードされ、CSメッセージの交換(ブロック270)が再試行される。

【0046】本発明の好適な実施例においては、マイクロプロセッサ・コントローラ620は、モトローラ社(アリゾナ州、フェニックス)製の2個のタイプ6303マイクロコントローラ・チップと、タイプDSP56001高速デジタル信号処理チップとから構成される。第1のタイプ6303のマイクロコントローラは、すべての信号流れタスクを行い、図4および図5の各々の段階をいつ行うかを決定し、第2のタイプ6303のマイクロプロセッサ・チップは、各メッセージ211、230、250、270の内容を判定し、タイプDSP56001のチップは、たとえばパブリック・キーに暗号化されたデータの暗号化と解読に関わる数値集約的な計算と、その他の同様の演算上の作業とを行う。モデム機能の好適な実施例はタイプV.26、あるいはタイプV.32である。これらのタイプのモデムは、モトローラ社の子会社であるUniversal Data Systems(アリゾナ州、Huntzville)により販売されている。しかし、その他のモデムや通信方法も用いることができる。

【0047】

【発明の効果】上記の説明に基づき、本発明が前述された問題を解決し、目的を達成して、しかも、とりわけここに示した実質的な利点を有することが当業者には明白であろう。その利点とは次のものである：(1)異なる

暗号化アルゴリズム、キー変数およびキー変数長を採用する異なる種類の機密データ通信用システム間で、複数の暗号化機関を含む単一の装置により、機密通信を行うことができる、(2)所定の階層のアルゴリズム、キー、通信モードなどを与えて、機密性を増大する、

(3)ユーザの目に見えないようにすることができる。これらの機能を1台の装置に備えることにより、本発明は装置の電源要件と費用とを最小限に抑えて、小型の装置を提供する。

【0048】本発明のもう1つの利点は、機密情報プロトコルとキー変数交換を自動化することにより、システムの操作に関するユーザの詳細な知識に対する必要性を最小限に抑えていることである。このために、機密通信用ターミナルの操作が簡単になる。さらに、システムの動作を記述する情報の配布に対する必要性が小さくなり、そのために詳細なシステムの知識の露出を最小限に抑えてさらに機密性が増す。

【0049】本発明は特定の要素、構造および段階に関して説明されたが、これらの選択は説明の便宜を図るためのもので、制限するためものではない。また、以上の説明に基づき、本発明は他の要素、装置および処理段階を選択した場合にも適用されることが当業者には理解いただろう。また、本開示に基づき当業者が考えられるであろう、本発明の範囲と精神とに入る上記その他の変形も、添付の請求項に含まれるものとする。

【図面の簡単な説明】

【図1】本発明による公共電話システムを用いた機密通信システムの概略図である。

【図2】本発明によるキー管理データ・ベースの概略図である。

【図3】本発明により機密通信を開始するためのメッセージ配列の一部の説明図である。

【図4】本発明の好適な実施例によるデータ速度と暗号化アルゴリズムの適合動作を示す流れ図である。

【図5】本発明の好適な実施例により機密通信を確立するための図3のメッセージ交換の一部をさらに詳細に示した流れ図である。

【図6】本発明の好適な実施例による機密通信用ターミナルの一例の概略図である。

【図7】本発明の好適な実施例による、送信および受信ターミナル間で交換されるメッセージにおいてキー発生機能を表わすビットの割当てを示す説明図である。

【符号の説明】

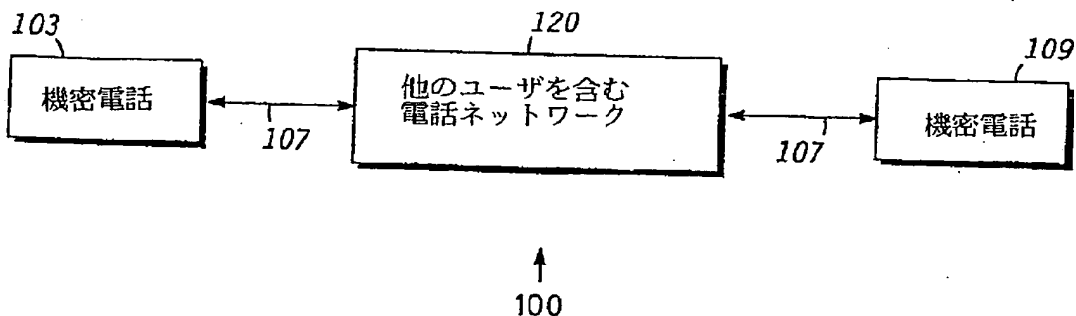
- 100 機密通信システム
- 103, 109 機密通信ターミナル
- 107 電話回線
- 120 電話ネットワーク
- 210 キー管理データベース
- 215 制御手段
- 220 相互接続部



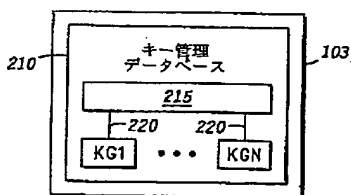
211 アクセス・ドメインおよび機能メッセージ  
230 認証メッセージ

250 乱数部メッセージ  
270 暗号化同期メッセージ

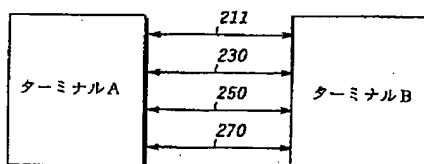
【図1】



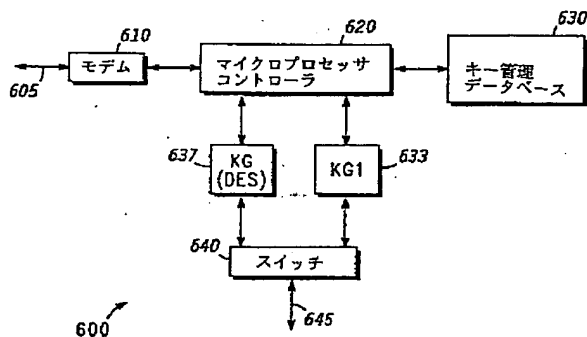
【図2】



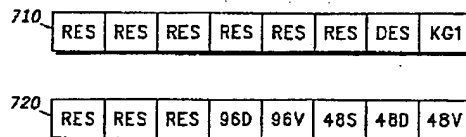
【図3】



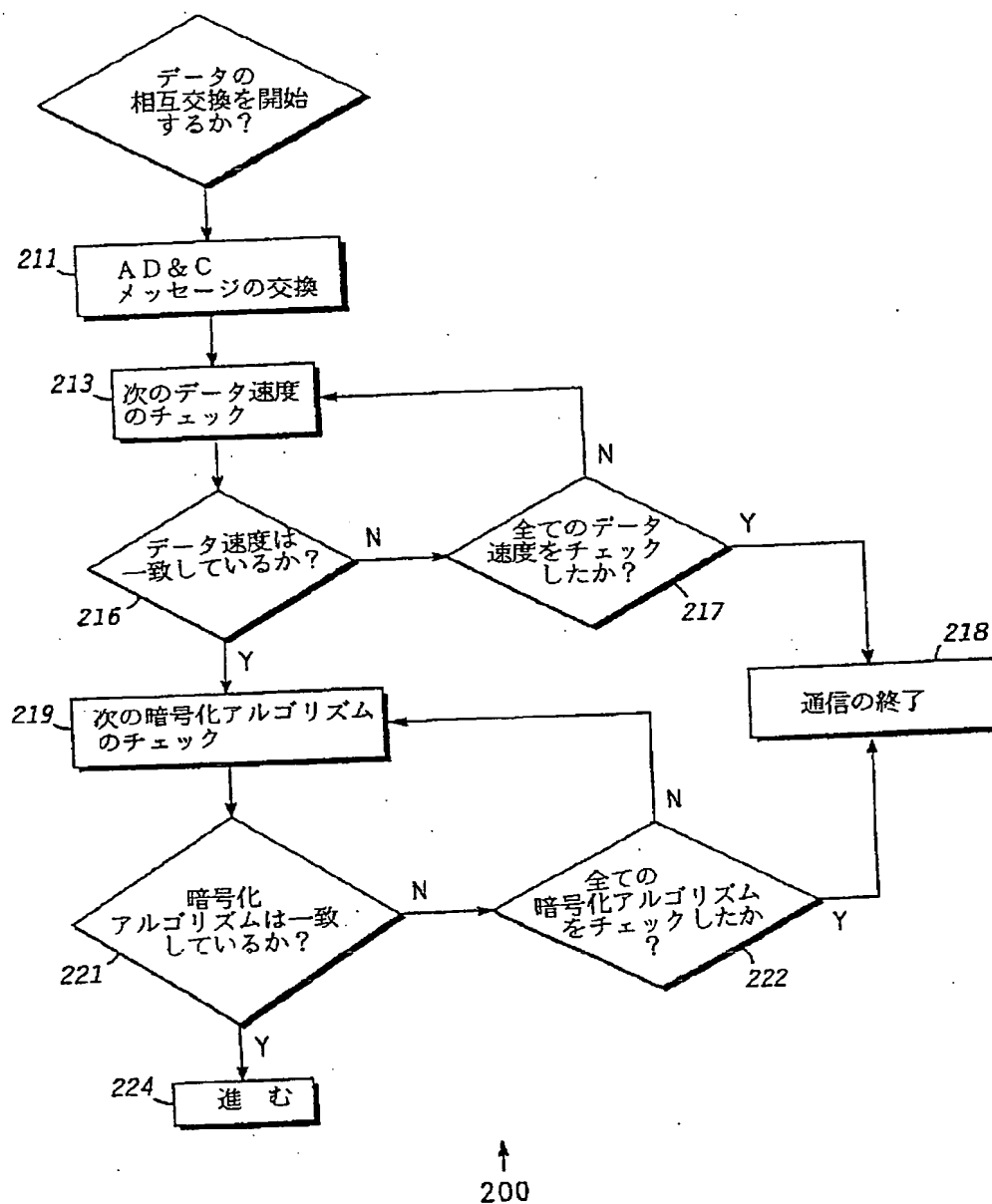
【図6】



【図7】



【図4】



【図5】

